Selecting a Standard Redundancy Method for Highly Available Industrial Networks

Hubert Kirrmann
ABB Corporate Research
Baden, Switzerland
hubert.kirrmann@ch.abb.com

Dacfey Dzung
ABB Corporate Research
Baden, Switzerland
dacfey.dzung@ch.abb.com

Abstract

Availability of Industrial Ethernet networks can be increased by providing redundant links and nodes. Although many specifications of Industrial Ethernet have been submitted to the International Electrotechnical Committee (IEC), they do not disclose methods to implement network redundancy. A working group of the IEC will, as part of the fieldbus maintenance team, issue guidelines for implementing redundancy in switched networks. Since the redundancy is dictated by the plant and less by the network, several solutions are studied.

While less time critical processes can be satisfied by a standby solution with alternate links, hard real time systems require a full duplication and parallel operation of redundancy. Both methods can be combined to increase further availability. Network safety or security is not considered here.

1. Introduction

Industrial Ethernet refers to the use of the Ethernet (IEEE 802.3) and Internet (in particular, TCP/UDP-IP) technologies to wire the automation system of industrial plants. Since the original goal of using cheap, off-the-shelf standard Ethernet components proved to be illusory, this technology was further developed for the industrial world by independent organizations. This resulted in a large number of competing specifications [1], [2], of which at least twelve have been submitted for standardization to the IEC. None of these specifications provides a scheme for redundancy. One reason is that many users trust that the redundancy issues have been tackled by the Ethernet specifications, and in particular by the RSTP [3] standard. Another reason is that it is not the network, but the controlled plant that dictates the redundancy requirements, and that different solutions may be valid. The IEC set up a working group to define redundancy schemes that can be applied to different Industrial Ethernet specifications. This paper gives classification and rationales behind redundancy solutions, some of which have also been described in [5].

2. Classification of plants

Before considering the control system and its data network, one should analyze the plant it is supposed to control. How long the plant can continue to operate after a complete or partial failure of its control system is a property of the plant, not of its control system. A failure of the control system normally does not have catastrophic consequences: a plant is designed with intrinsic protections against failures of the control system, for instance relief valves or flywheel brakes. However, upon detection of a failure, and to avoid damages, a plant takes actions such as emergency shut-down, fall-back mode or reversal to manual operation, which causes loss of production. To avoid this, the automation system should resume operation before the plant takes actions. The time that the plant allows for recovery before taking such emergency actions is the grace time.

One distinguishes different kinds of plants (A,B,C) depending on the grace time:

All-round: grace time < 2 s

soft real-time, such as building automation, process industry, where human interaction and manual repair are possible.

Benign plants grace time< 50 ms

real-time, such as chemical industry, power plants, manufacturing

Critical plants: grace time < 2 ms

hard real time, such as synchronized drives, printing, robot motion control, X-by-wire for the automobile industry.

Example: at 144 km/h, a car travels 4 cm / ms, the steering angle can move 2000° / s. If steering is computer-controlled (Drive-By-Wire) and full steering is inadvertently applied, in the worst case the car can be off-track by 5 cm within 5 ms. This is the time allowed for recovery in case of control system failure.

Obviously, network recovery delay in case of failure must be shorter than the grace time to pass unnoticed by the application.

3. Redundancy requirements

Which solution to choose and which amount of redundancy is needed depend on several requirements:

Recovery delay
: The duration of loss of service in case of failure until service is restored must be lower than the grace time.

Degree of redundancy
: The quantity (full, partial replication) and type of redundant components that are allowed to fail with no loss of service must be matched against the economical objectives.

Graceful degradation
: Redundant resources can be lowered if partial system loss is acceptable, provided faults are correctly isolated.

Behaviour when failing
: System that offer a safe state can rely on fail-silent components, while systems without such must tolerate uncontrolled sending during a certain time.

Supervision
: Redundancy is useless unless supervised (avoid lurking errors). Even intermittent failures must be reported as a measure of system health.

Reintegration time
: The duration of disruption to restore redundancy after (manual) repair should not exceed the grace time, except when planned maintenance is suitable.

Economical advantages of decreased mean time between unscheduled repairs must be weighted against the economic costs of redundancy – provided maintenance can be deferred.

Economic advantages of redundancy in terms of higher availability (productivity) must be weighted against decreased mean time between failure (redundant components also fail).

Hardening components and better maintenance teams increase availability, but this is not considered here.

4. Device and network redundancy

To clarify the following, it is important to distinguish device and network redundancy. The network is drawn as a bus for simplicity, but it can be – and usually is - a switched network as well.

Device duplication in this context is for the purpose of functional redundancy. Device duplication for the purpose of error detection – as is common in the safety community – is not considered here.

Control systems may exist in which critical devices are duplicated, but the network is not, as Figure 1 shows. This is a solution often found in safety-oriented systems, which are not considered here.

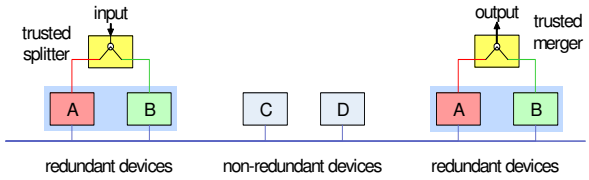

Figure 1: Duplicated devices, single network

Other solutions, as Figure 2 shows, consider that the critical control system is duplicated, each half owning its devices and networks, under the assumption that both control systems will not fail at the same time. Such a solution is used where a very high availability is sought.

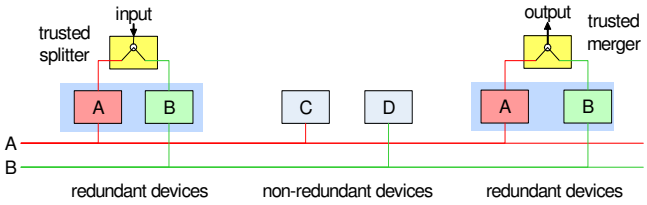

Figure 2: Duplicated devices, segregated networks

An even higher availability can be achieved if the redundant devices are connected to both redundant networks, as Figure 3 shows. In practice, such architecture only brings benefits where the mean time between repairs is very high.

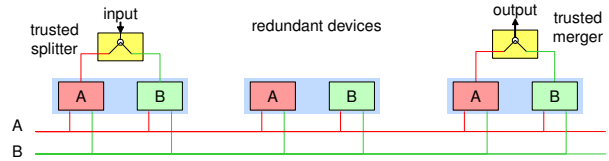

Figure 3: Duplicated devices attached to both networks

In the following, we will consider only network duplication, the network is not aware that some devices (e.g. A and B) form a redundant pair, as Figure 4 shows.

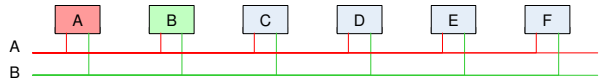

Figure 4: Non-redundant devices attached to a redundant network

Considering a single device, redundancy can be introduced at any level in the communication stack, as Figure 5 shows. The different solutions distinguish themselves by the number of IP and MAC addresses that must be managed.

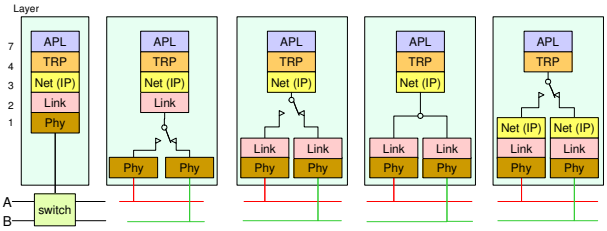

Fig.5: Levels of redundancy

5. Classification of redundancy methods

The following considerations apply both to network and to processing elements. Continued operation requires a functional redundancy, i.e. a second device capable of executing the function of a failed device. There exist two fundamental functional redundancy methods, dynamic and static redundancy, as Figure 6 shows.

5.1. Dynamic redundancy (standby)

Functional redundancy is normally idle or performs other tasks. It is switched in when needed. Redundancy does not participate in the function; a switchover logic selects the operating computing or communication channel

Advantages:

+ shares redundancy (one standby can serve several on-line units)
+ reduces failure rate of redundancy (if standby is inactive)
+ reduce common mode errors (since the on-line unit and standby fail independently)

Drawbacks

- switchover takes time
- redundancy is not continuously exercised; therefore, latent, undetected faults may develop.
-synchronization nevertheless needed

5.2. Static redundancy (massive redundancy, workby)

Both functional redundancies participate in the function; the plant chooses the trusted communication or computing channel(s). The plant may just use both channels (i.e. each channel operates an actuator) and/or the plant may rely on plausibility information (error detectors) to isolate a suspect channel.

Advantages:

+ switches over smoothly
+ continuously exercises redundancy and therefore increases error detection coverage
+ could be used as a mean to detect errors by comparison, as a way to provide fail-silent behaviour (not considered here)

Drawbacks

- costs a total duplication
- requires synchronization.

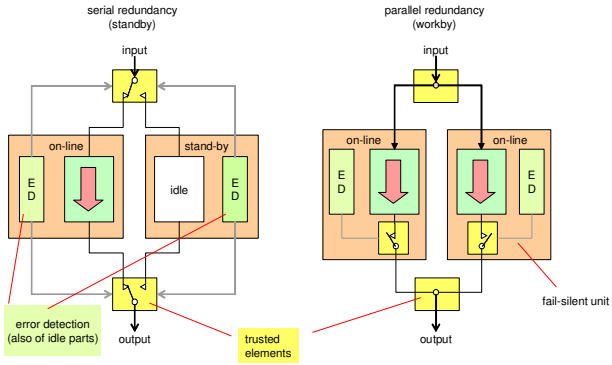

Fig. 6 .The two main principles of redundancy: standby or workby

Both methods work under the premise that the errors are detected in useful time by some error detector (ED) and that switchover is successful.

The major difference in real-time systems – and the one that counts in this context - is that standby redundancy always requires a non-zero switchover time while workby redundancy can be bumpless, if the plant has the ability to cope with both channels or to operate with only one.

Note: the terms “static” and “dynamic” redundancy are accepted in the fault-tolerance research community, although it may sound strange that the static redundancy is quite dynamic and the dynamic redundancy can be passive (cold standby) when not used.

6. Standby redundancy in networks

Networks traditionally rely on (hot or warm) standby. In case of disruption, the packets seek a new path in the network. This has been the principle since the Arpanet existed.

Figure 7 shows a typical Industrial Ethernet network consisting of switches and links.

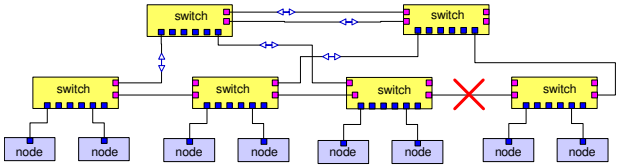

Fig. 7: Network with redundant paths and devices with single attachment.

In case of link failure (cross in Figure 7) the switches reroute the traffic over the remaining paths. This operation is typically performed according to the RSTP (Rapid Spanning Tree protocol, IEEE 802.1D [3]. The above scheme shows the nodes and switches as separated devices, but the principle does not change if switch elements are integrated into the nodes. RSTP supports general network topologies; recovery may require hundreds of milliseconds. Where the network is restricted to redundant rings, faster recovery schemes have been proposed and implemented, see e.g. [4].

RNRP has a non-negligible switchover time, in the order of several seconds. Clever implementations can reduce this time to below one second, e.g. by calculating beforehand all alternative links and recalculating the tables instead of reinitializing the network to transparent mode.

In a variety of industrial networks, a simplified version of RNRP exists as a double-ring topology in which link failures are overcome by reconfiguring one node in the ring (Figure 9). Since topology is known, reconfiguration takes only a dozen of milliseconds – one order of magnitude faster than RNRP. While this method increases availability in face of link failures, it provides only graceful degradation – loss of functionality – in view of switch failures.

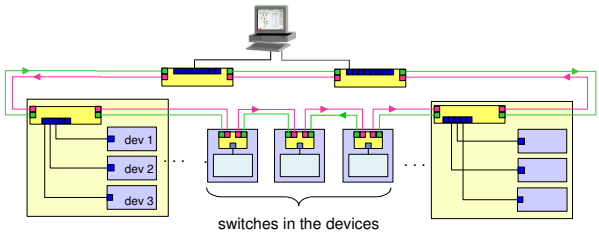

Fig. 8: Double ring redundancy

To cater with switch failures, a node should be attached to two switches (operator workstation in Figure 8). This calls for a switchover logic in nodes attached to two switches. While a switch element obeying RSTP could be inserted in each device, the switchover times would degrade to what RSTP offers.

In its simplest form, the switchover logic can be included in each device, as Figure 9 shows for a standby redundancy at the physical level. Note the liveliness supervision that checks that the redundancy is still operable. Here also, switchover is not instantaneous since each node must discover the failure of the switch or link and reroute traffic over the remaining link. Nevertheless, switchover is fast enough to remain unnoticed by benign applications.

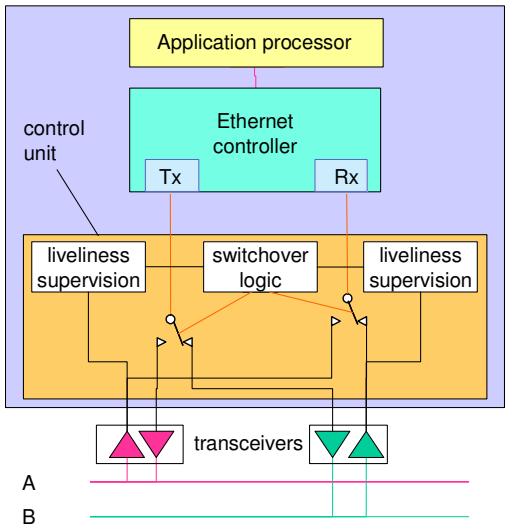

Fig. 9: Standby at the physical layer

7. Workby redundancy

To achieve a very fast switchover, it is necessary to operate the redundant network in parallel (Figure 10). The principle of operation is “send on both, receive from both”. The receiver decides which line to trust, or in case both lines are trusted, which frame to ignore.

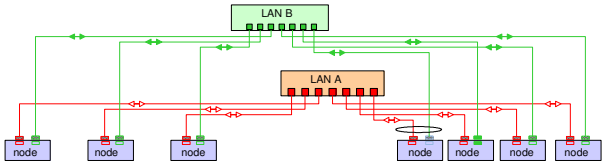

Fig. 10: Two networks operated in parallel

In each device, both channels work in parallel. Rejection of duplicates can be taken care of by the network protocols. Indeed, TCP communication is designed to reject duplicates, and applications basing on UDP must be designed to tolerate duplicates, since UDP cannot guarantee freedom of duplicates.

Many Industrial Ethernet networks also operate with a publisher /subscriber scheme based directly on layer 2. Fortunately, the publisher / subscriber scheme allows for duplicates, indeed, reception of duplicates increases the robustness.

To offload the processor, it may be advantageous to let the network controller filter duplicates at the link layer – network layer filtering fails because some publisher / subscriber protocols operate on layer 2 only.

Figure 11 shows a node with static redundancy that filters duplicates in a merge layer on top of the link layer.

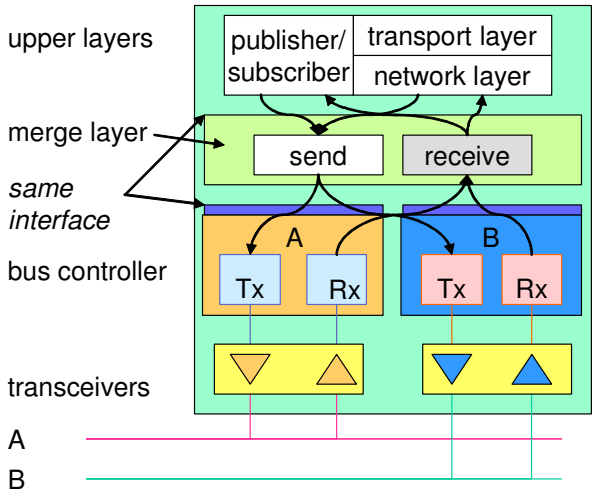

Figure 11 Principle of workby in a node

This method offers bumpless switchover, and an increased resiliency in view of spurious network errors, at the cost of doubling the hardware and requiring an intervention in the devices (special drivers), that may be cumbersome for standard PCs, for example. This problem is however the same as with double-attached devices operating with standby links.

Since one cannot expect all devices to be attached to both networks, a solution must be found to integrate single attachment devices. Here, several protocols exist that allow to identify which devices operate on both LANs or on one LAN only.

8. Recommendation for standardization

The above shows that there exist different classes of plants that can accept different redundancy methods, which al have their advantages and disadvantages. There exist numerous redundancy scheme on the market that operate according to the above mentioned methods. The objective of standardization is to reduce the number of solutions to a handful so as to ensure interoperability. A standard redundancy solution shall:

1. Be independent of the higher protocol used
2. Be compatible with existing equipment, especially commercial PCs and switches, where no redundancy is used
3. Define the layout rules and especially the integration of different levels of redundancy
4. Define means to supervise the redundancy, e.g. using SNMP
5. Define scenarios for life insertion and reintegration of repaired components
6. Define measurable performance goals, such as switchover times and reintegration time
7. Specify, if several solutions emerge, their (distinct) application domains and recommendation for their use must be stated.

9. Conclusion

The Industrial Ethernet community would best be served by standardizing on only three types of redundancy:

all-round plants with no special timing requirements can be served by the classical RSTP protocol that is already standardized (801.1D);

benign plants that can't tolerate more than 500 ms range can rely on a redundant ring structure with deterministic recovery time, and

critical plants whose grace time lies below what the redundant ring can provide require a workby redundancy that bases on parallel operation of networks.

References

[1] Felser, Max, "Real-Time Ethernet – Industry Prospective," in Proceedings of the IEEE, VOL. 93, NO.6, June 2005

[2] http://www.real-time-ethernet.de/

[3] Rapid Spanning Tree Protocol, IEEE standard 802.1D

[4] Extreme Networks, Ethernet Automatic Protection Switching (EAPS), RFC 3619.

[5] Kai Hansen, "Redundancy Ethernet in Industrial Automation", 10th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2005, Catania, Italy, 19 - 22 September 2005, Proceedings, Vol.2, pp.941-947.